Device for protecting the first use of a processor smart card

This invention relates to a method for protection from attacks on a processor smart card or from its unauthorized use in a network for communication, preferably a GSM network, according to the preamble of claim 1, and to a corresponding smart card according to the preamble of claim 9.

In GSM systems it is known that for using the smart card (Subscriber Identity Module SIM) the card user must first identify himself as a legitimate user by means of a Personal Identification Number (PIN). To avoid abuse at this point it is known to transmit the PIN to the card user by having PIN/PUK letters produced by the card manufacturer or card personalizer and handing over said PIN/PUK letters to the card user.

Another, system-relevant security measure is the sealing of the PIN/PUK letter by the card manufacturer or card personalizer. The intactness of the seal on the PIN/PUK letter indicates to the card user that the secret numbers applied to the PIN/PUK letter by the card manufacturer cannot be known to any other card user. Since the secret numbers on the PIN/PUK letter were chosen randomly by the card manufacturer or card personalizer and are stored only in the secret memory of the SIM card, the card user can assume that by opening the PIN/PUK letter only he himself acquires knowledge of the secret numbers.

To avoid abuse upon PIN entry, it is known for PIN entry to provide an error counter that temporarily prevents further use of the card when a permissible number of abortive attempts is exceeded. To protect from unnecessary blocking of a card by inadvertent false entry of the PIN, it is known to provide on the card a Personal Unblocking Key (PUK) which can be used to define a new PIN and which reenables the card for use in the network. To avoid abuse upon PUK entry, it is known to provide an error counter which definitively prevents further use of the card when a permissible number of abortive attempts is exceeded.

In the known prior art, the card user is given the possibility of replacing the PIN defined by the card manufacturer or card personalizer by a self-chosen value. The value of the PUK cannot be changed by the card user. To be able to inform the card user of the PUK if the PIN/PUK letter is lost or inaccessible but the PIN inadvertently blocked, it is known to store the PUK additionally in a data base centrally with the network operator for all issued cards as a special service in some GSM networks. At the card user's request and after a check of the card user's identity, the PUK is transmitted to the card user for enabling the PIN.

Such a system also involves the danger that, by unauthorized opening of the PIN/PUK letter and for example by reprinting of the PIN/PUK letter or by manipulation of the PIN/PUK letter seal, the legitimate card user believes that he is the first user of the card although an illegitimate card user has already put the card into operation temporarily at the expense of the legitimate card user.

It is therefore the problem of the invention to provide a safe method for protection from unnoticed opening of PIN/PUK letters by which the first user of the card is notified of the first use of the card, as well as a corresponding smart card.

This problem is solved starting out from the features of the preambles of claim 1 and 9 by the respective characterizing features. Advantageous embodiments of the invention are stated in the dependent claims.

The invention relates to a method for checking and displaying the first use of a processor smart card by means of an additional application on the processor smart card itself which controls or at least substantially influences all steps necessary for a safe check.

An advantageous embodiment of the invention shows the use of the application to let the card user define secret keys required for authentication of the card user with respect to the card, or to transmit said keys to the card user, whereby the card remains transport-protected on the way between card manufacturer, card issuer and card user.

Another advantageous use of the invention is the supplementing or replacement of elaborate and sometimes cost-intensive methods for transport protection of processor smart cards between card manufacturer and card user, for example PIN/PUK letters, by the additional application in the processor smart card which supplements or substantially performs the function of a PIN/PUK letter.

According to another advantageous embodiment, the invention can also be used as a component of a system executed in essential parts in the processor smart card itself for individual allocation and personalization of secret keys which are to be made accessible not only to the card user but also to the card issuer, e.g. a mobile phone network operator or network service provider.

Another advantageous embodiment of the invention provides that when the secret keys are defined by the card user himself, said secret keys are asked for several times by the card user in order to avoid inadvertent false entry.

Alternatively or additionally, after the secret numbers have been defined by the card user or by the card itself a corresponding network component can be sent a message after which the first use of the card in the network is communicated or the value of the secret number transmitted.

According to another advantageous embodiment of the invention, when the card is first put into operation the secret numbers are additionally or alternatively inputted or outputted via the speaking or hearing apparatus of the mobile phone device, which can in particular facilitate and better protect the transmission or definition of secret keys to or by visually handicapped card users.

Fig. 1 shows an example of smart card *SIM* having interface *S* for data exchange with a mobile phone and microprocessor *µP* connected with application *A* and memory *M*, *Mg*. Application *A* can be formed substantially as a SIM Application Toolkit application and has been incorporated into the card by the card manufacturer or card personalizer. The memory is divided into usual memory area *M* where data can be read and written, and secret memory area *Mg* where at least the information about the first use of the smart card is stored. When the card is put into operation by a card user via interface *S*, the application checks by accessing secret memory *Mg* whether this is the first use of the card.

Upon the first use of the card, the card user is informed by application *A* and asked to confirm the putting into operation of the card. Upon positive confirmation by the card user, the application changes the information about first use in secret memory *Mg*, thereby changing its behavior when the card is put into operation again later.